Remarks/Arguments

Reconsideration of the Application is requested.

Minor portions of the Specification have been amended to be more accurate.

Claims 1-32 have been rejected by the Examiner under 35 USC 1.02 (b) as being clearly anticipated by Montgomery et al. (U.S. Patent Publication No. 2003/0101143).

Montgomery discloses the following in paragraph [0006].

> "[0006] Thus, the date (item #7) embedded in the barcode portion of the postage indicium 104 could be compared to the current date, as well as to the human-readable date. The postage amount (item #6) embedded in the barcode portion 106 of the postage indicium 104 could be compared to the human-readable postage amount and for United States addresses, the delivery point ZIP code (item #9) embedded in the barcode portion 106 of the postage indicium 104 could be compared with the delivery address 114 printed on the mail piece 100, Should any of these "information pairs" show an inconsistency, the mail piece 100 would be immediately suspect and would be a candidate for further investigation."

Montgomery is comparing the postal amount embedded in the barcode portion of the postal indicium with the human readable postal amount and the delivery point zip code embedded in the barcode portion of the postal indicium. The amount of postage and the zip code are data that are known to the mailer.

The comparison of data is only viable if one is comparing data from two different sources. Montgomery does not prevent fraud since the mailer may use data which he knows from the same source i.e. the postage amount and zip code on the face of the mail piece.

Montgomery discloses the following in paragraphs [0034-0038].

> "[0034] Unlike the two dimension IBI postage indicia barcodes, these standard tracking ID's (which are generally represented in simpler one dimensional barcodes, such as Code 128, Code 39, etc) are typically scanned 100% of the time. This scanning is a result of the normal processing that the postal authority implements to keep track of mail pieces (typically packages), and thus any

copyist that duplicates the postage indicium would not be able to correspondingly copy the standard tracking ID's without detection of duplicated tracking ID's or at least a tracking ID that is outside a normal range of tracking ID's. Thus, a comparison between the tracking ID found in the self-validating postage indicium and the standard tracking ID would reveal a discrepancy and thus possible fraud. This approach would be very effective in the case of two packages going from the same sender to the same destination address. While both packages would have the same delivery ZIP+4+2 (a potential copy attack described earlier in this specification), the packages would have different tracking ID's. The copyist would be further frustrated in his attempt to copy an existing valid indicium and tracking ID pair, and use that matched pair on another package altogether. This type of fraud would very likely be detected by the routine delivery scans of the tracking ID performed by the postal authority.

[0035] In accordance with a first aspect of the present inventions, a method of providing a unique postage indicium within a postal system (e.g., the USPS) is provided. The method comprises generating a unique postage indicium having a character string (such as, e.g., a tracking ID) that is unique within the postal system. The tracking ID can be obtained from a single database to ensure its uniqueness. In addition to the unique tracking ID, the postage indicium can contain a number of other items, such as, e.g., indicia version number, algorithm identification, certificate serial number, device identification, ascending register, postage, date of mailing, originating zip code, software identification, descending register, and rate category. The method further comprises deriving a digital signature from the unique tracking ID, and associating the digital signature with the unique postage indicium to generate a self-validating unique postage indicium. In the preferred method, the digital signature is generated by applying a private key to the unique postage indicium. The digital signature is then attached, e.g., by appending, to the unique postage indicium. This self-validating unique postage indicium can then be applied to a mail piece (such as, e.g., a package or envelope) in a barcode format. The unique tracking ID can also be applied to the mail piece independently of the self-validating unique postage indicium, as is the typical case with tracked packages.

[0036] In accordance with a second aspect of the present inventions, a method of detecting postal fraud in a postal system (such as, e.g., the USPS) is provided. The method comprises receiving a plurality of mail pieces within the postal system, each

carrying a self-validating postage indicium having a character string (such as, e.g., a tracking 10) and a digital signature derived from a data stream that includes the tracking ID, and optionally other postage related data.

[0037] The method further comprises reading each self-validating postage indicium to obtain the postage indicium and digital signature, validating each postage indicium by determining if the digital signature is consistent with the tracking 10, and if applicable, the associated indicium data, and comparing all of the tracking !D's obtained system-wide from the postage indicia. Thus, postal fraud can be detected if two of the unique character strings (e.g. tracking ID's) match. In the preferred method, each self-validating postage indicium is embodied in a two dimensional barcode format that can be read with a barcode reader. Each digital signature can be generated with a private key, in which case, the postage indicium authentication comprises applying a corresponding public key to each digital signature.

[0038] In accordance with a third aspect of the present inventions, a method of detecting postal fraud in a postal system (such as, e.g., the USPS) is provided. The method comprises receiving a mail piece within the postal system, wherein the mail piece carries a self-validating postage indicium having a character string (such as, e.g., a tracking ID), and a digital signature derived from a data stream that includes the tracking ID, and optionally other postage related data. The mail piece further carries an expected representation of the same tracking ID independent of the self-validating postage indicium. It is customary that this latter representation consists of a human readable string plus a one-dimensional barcode representation of that string. The method further comprises reading the self-validating postage indicium to obtain the postage indicium data and associated digital signature, validating the postage indicium data by determining if the digital signature is consistent with the tracking ID, and comparing the validated tracking ID obtained from the postage indicium to the tracking ID found elsewhere on the mail piece. Thus, postal fraud can be detected if the tracking ID obtained from the postage indicium does not match the expected representation of the tracking ID found elsewhere on the mail piece, indicating that the postage indicium has been duplicated. Postal fraud can further be detected if two or more of the tracking ID's found on two or more mail pieces match each other, indicating that the tracking ID's have been duplicated to match the duplicated postage indicium. In the preferred method, each self-validating postage indicium is

> embodied in a barcode format that can be read with a barcode reader. Each digital signature can be generated with a private component of a key pair, in which case, the postage indicium authentication comprises applying a corresponding public key to each digital signature."

Montgomery adds the standard tracking ID's to the protected portion of the indicia. Then in the verification environment Montgomery records that he saw the tracking ID on the mail. If Montgomery notices the same tracking ID again on different mail, Montgomery knows fraud has been committed.

Montgomery does not disclose or anticipate the invention claimed by Applicant in claim 1. Namely, Montgomery does not disclose or anticipate the steps of a and e of claim 1, obtaining a digital image of said other printed material and generating characterizing information descriptive of aspects of said image, said aspects being selected from the group consisting of, lengths of elements of said image, numbers of outliers in said image, and shapes of said image or of elements of said image, said characterizing information being selected to fit within said indicium; said object's relationship to said indicium can be verified by regenerating said characterizing information from said other printed material and comparing said regenerated characterizing information with characterizing information recovered from said indicium, and copies of said indicium cannot easily be used without detection on other objects which do not include said other printed material.

Montgomery also does not disclose or anticipate steps b and d of claim 17. Namely, a processor for receiving a digital image of said other printed material, and for processing said image to abstract characterizing information descriptive of aspects of said image from said image, said aspects being selected from the group consisting of, lengths of elements of said image, numbers of outliers in said image, and shapes of said image or of elements of said image, said characterizing information being selected to fit within said indicium; said object's relationship to said indicium can be verified by regenerating said characterizing information from said other printed material and comparing said regenerated characterizing information with characterizing information

recovered from said indicium, and copies of said indicium cannot easily be used without detection on other objects which do not include said other printed material.

In step a of claim 1, applicant obtains a digital image of said other printed material (the address block) and generates characterizing information descriptive of aspects of the address block. The aspects may be the lengths of elements, numbers of outliers and shapes in the address block. A manner in which the foregoing may be accomplished is shown in Fig. 3 and described in paragraphs [0026]-[0034] of the specification. The characterization of the information created by applicant from the address block is robust in view of data that may be produced by mailers and retrieved in the postal verification process.

In step e of claim 1, applicant verifies the characterizing information by comparing the regenerated characterizing information with characterizing information recovered from the indicium. Thus, copies of the indicium cannot be easily made without detection on other mail pieces that do not have the exact same address block.

Applicant's unique characterization of the address block is easily and economically extractable by the mailer and during postal verification the characterization of the mail piece address block can be independently reproduced and verified by the post. Whereas, Montgomery creates a unique characterization of the mail piece within the postal system by adding a tracking ID to the mail piece.

Please charge any additional fees that may be required or credit any overpayment to Deposit Account Number 16-1885.

In view of the above claims 1-32 are patentable. If the Examiner has any questions would the Examiner please telephone the undersigned at the number noted below.

Respectfully submitted,

/Ronald Reichman/
Ronald Reichman
Reg. No. 26,796
Attorney of Record
Telephone (203) 924-3854

PITNEY BOWES INC.
Intellectual Property and
Technology Law Department
35 Waterview Drive
P.O. Box 3000
Shelton, CT 06484-8000